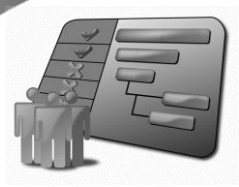

WBS framework

Estructura de trabajo para implementar la Ciberseguridad en la industria de Petróleo y Gas

ZONES & CONDUITS MANAGER

ASSESS

START HERE

SUC — Identificación completa del Sistema en consideración

GAP — Estudio GAP & Maturity, y Evaluación de CSMP
Ref. DOE C2M2 for Oil & Gas, INGAA Pipelines

HLRA — Análisis de riesgos de alto nivel
Ref. ISA/IEC-62443-3-2

CPHA — Análisis detallado de la ciberseguridad industrial
Ref. ISA/IEC-62443-3-2

Organizaciones Soportadas:

ISA · INGAA

Las inversiones en seguridad están justificadas con una metodología sólida científica de evaluación de riesgos

IMPLEMENT

START HERE

CDZC — Diseño Conceptual de Zonas y Conductos
Ref. ISA/IEC-62443-3-3, INGAA, NIST Controls

CSRS — Especificación de requisitos de seguridad cibernética
Ref. ISA/IEC-62443 Foundational Requirements

ACRA — Diseño e Implementación de Control de Acceso y Acceso Remoto
Ref. ISA/IEC-62443-3-3, NERC and NIST Controls

IFDI — Diseño y implementación de cortafuegos industriales

- ✓ Comprensión plena de todos los componentes cibernéticos, que pueden ser comprometidos.
  - La capa tecnológica.
- ✓ Análisis integral de las fortalezas y debilidades de la organización a través del estudio de mejores prácticas, incluyendo GAP y análisis de madurez con C2M2.
  - La capa de gobierno.
- ✓ Comprensión completa de los activos para proteger, identificación de receptores de riesgo, todas las posibles consecuencias y sus impactos con los estudios HAZOP.
  - La capa física.
- ✓ Cálculo del Riesgo de Ciberseguridad Industrial a través de la metodología RAGAGEP para tomar las mejores decisiones que realmente mitiga todo el riesgo intolerable de ciberseguridad.
- ✓ Priorizar todo tipo de amenazas, que pueden comprometer cualquier componente cibersensible, incluyendo naturales, entidades y tecnología.
- ✓ El nivel de seguridad (SL-T) es determinado por cada nodo (Zona y conducto) dentro de la capa tecnológica.
- ✓ Se produce una lista completa de recomendaciones (procesales, tecnológicas y físicas) en el diseño de nuevos sistemas o el rediseño de los sistemas existentes que realmente mitiga todos los riesgos.
- ✓ Todas las recomendaciones están diseñadas en las tres capas de forma coherente con otras disciplinas de riesgo industrial, entre otros requisitos de seguridad y cumplimiento. Diseño detallado y priorización de mitigaciones y contramedidas con NIST.
- ✓ Cada Nodo produce una especificación de requisitos de ciberseguridad, según cada SL-T, para nuevos sistemas futuros, antes de comprar cualquier cosa.
- ✓ Implementación de las políticas de control de acceso y acceso remoto en el IACS de forma coherente con los SL-T utilizando los controles NERC-CIP y las guías de NIST.
- ✓ Implemente la seguridad del switch, del router, del concentrador y del firewall y la segmentación de la zona de acuerdo con los SL-T.

El WBS WisePlant con ZCM proporciona un enfoque modular fácil y rápido que realmente funciona. ¡Comience a invertir ahora!

IMPLEMENT

CAT — Prueba de Aceptación Cibernética del IACS
Ref. ISASecure

ISASecure®

- ✓ Realizar Cyber-FAT (Prueba de Aceptación de Fábrica) en nuevos sistemas antes de que se entreguen a la planta para validar y confirmar que cumple con CSRS y SL-T requeridos.
- ✓ Realizar Cyber-SAT (Pruebas de Aceptación del Sitio) y Prueba de Robustez de Laboratorio para validar los Requisitos del seguridad e identificar nuevas vulnerabilidades en los Ciber-Assets más críticos.

HARD — IACS y endurecimiento de la red industria
Ref. NIST & ISA Guidelines

- ✓ Realizar el endurecimiento de Cyber-Assets and Assets para reducir la superficie de ataque, de acuerdo con las definiciones SL-T y las recomendaciones del fabricante.

PMI — Project Management & Mitigations Implementation
Ref. PMBOK

- ✓ Implementar todos los medios de reducción de riesgos a través de mitigaciones recomendadas (procedimiento, tecnológico y físico).

Si llegó aquí, ya está ejecutando su planta en (o por debajo) del riesgo tolerable, y en la zona de seguridad de acuerdo con otras disciplinas de riesgo industrial. Los Activos están fuera de riesgo y el riesgo de ciberseguridad industrial se mitiga.

Muchos proveedores de seguridad que utilizan el enfoque de TI tradicional (seguridad de la información) están saltando directamente aquí, con la metodología de evaluación de riesgos incorrecta, generando una gran cantidad de eventos – falsos positivos – sobrecargando la capacidad de la organización para responder, sin realmente valorizar los Activos para Proteger y sin mitigar los riesgos de ciberseguridad industrial. No existe una "solución mágica" para la ciberseguridad industrial!

START HERE

OTMO — Monitoreo pasivo y no intrusivo de IACS y redes industriales
Ref. NIST, ISA/IEC-62443

- ✓ Implementar la supervisión de la detección de intrusiones y anomalías basada en definiciones SL-T a lo que más importa y la priorización de amenazas, para prevenir las amenazas actuando sobre la organización para comprometer los componentes cibersensibles.

SOCOT — Operación de SIEM & SOC para inteligencia de OT
Ref. NIST, ISA/IEC-62443

- ✓ Implemente el sistema de gestión de la seguridad de la información y los eventos (SIEM) integrado de forma inteligente con los sistemas de gestión de alarmas de plantas para responder rápidamente a las acciones de amenazas y proteger lo que realmente importa.

MAINTAIN

MOCP — Gestión de los Procedimientos de Cambio
Ref. ISA/IEC-62443

- ✓ Evalúe los cambios con una metodología fiable de evaluación de riesgos coherente antes de introducir cambios en el SuC/EuC garantizando una transición sin problemas en la planta.

PMDS — Actualizaciones & Servicio de Administración de Parches
Ref. ISA/IEC-62443-2-4, NIST

- ✓ Evaluar la criticidad de cada actualización o parche proporcionado por los proveedores equilibrados con los riesgos asociados y SL-T. Clasificar los descubrimientos a medida que se reciben del CERT.

BURS — Programa y Servicio de Copia de Seguridad y Restauración
Ref. NIST, ISA/IEC-62443

- ✓ Implementar sistemas y procedimientos de respaldo y restauración.

PCSA — Auditorías periódicas de ciberseguridad del IACS
Ref. NIST, ISA/IEC-62443

- ✓ Realizar auditorías periódicas de ciberseguridad industrial para el cumplimiento y encontrar oportunidades de mejora.

Los sistemas de control permanecerán en la planta por lo general durante +20 años. Este es el viaje más larga. Por lo tanto, vamos a hacer que sea agradable y cómodo, para una Operación y Mantenimiento de la planta a dentro del riesgo tolerable. <u>No se pierda los dos primeros viajes</u>.

GET MORE INFO